REMARKS

Claims 2-85 are pending in this application. Claim 1 has been previously cancelled. By this paper, the Applicant amends claims 2 and 73. No new matter has been added.

At paragraph 4 of the Office Action, the Examiner rejects claims 2-72 under 35 U.S.C. §102(a) as being anticipated by Secure Computing Corporation: "Authentication Reference Guide," XP-002283680, pp. 1-18, September 4, 2002 (Secure Computing). (Although the Examiner has cited the publication date of this reference as "April 9, 2002," the Applicant believes this to be incorrect. The front page of this document shows September 2002, and the bottom of each subsequent page shows "09/04/02." Therefore the Applicant respectfully submits that the publication date of this document is September 4, 2002). The Applicant traverses this rejection.

At paragraph 5 the Examiner allegedly identifies specific text in Secure Computing that teaches elements of independent claims 2, 26, 43 and 57. The Examiner incorrectly states that these claims include the limitation:

> generating an identity authentication code that depends at least in part on (i) a dynamic
> value, (ii) the event state, and (iii) a secret associated with he device.

However, claims 2, 26, 43 and 57 do not include this limitation. None of these claims recite "a dynamic value." Each of these claims includes the following limitation:

> generating an identity authentication code that depends on (i) the event state data, and (ii) a
> secret associated with the device.

Claims 2, 26, 43 and 57 differ in how the term "the event state data" is characterized. Claim 2 recites:

> providing event state data that specifies a condition of the authentication device

Claim 26 recites:

> providing event state data that is a security indicator for an authentication system of which
> the authentication device is a component

Claim 43 recites:

> providing event state data that specifies information about a user of the authentication device

Claim 57 recites:

> providing event state data that specifies information about environmental conditions
> associated with the authentication device

Regarding the "event state [data]", the Examiner cites pages 11-12 and 14-16, "response" of Secure computing as teaching this claim element. The Applicant respectfully submits that the "response" from Secure Computing pages 11-12 and 14-16 has no relationship to "the event state data" as recited in claims 2, 26, 43 and 57. In particular, Secure Computing teaches that the "response" is a result of the authenticator operating on a random number challenge (page 14). Secure Computing does not teach or suggest that the "response" has any relationship to any condition of the authentication device (as in claim 2). Further, Secure Computing does not teach or suggest the "response" having any relationship to a security indicator for an authentication system of which the authentication device is a component (as in claim 26), or that specifies information about a user of the authentication device (as in claim 43), or that specifies information about environmental conditions associated with the authentication device. For clarification, the Applicant amends claim 2 to recite:

> providing event state data <u>representing an occurrence of a reportable event concerning</u> ~~that~~
> ~~specifies~~ a condition of the authentication device

This amendment is supported throughout the specification, for example at paragraph [0011]. This amendment clearly excludes the "response" of Secure Computing, since a "reportable event" is an event other than events associated with the normal operation of an authentication method. The event state data of claims 26, 43 and 57 are clearly other examples of such reportable events. Thus, the identity authentication code of claims 2, 26, 43 and 57 is based on information about reportable events (i.e., the event state data), in addition to the conventional inputs for a response computation.

Secure Computing does not teach or suggest such an identity authentication code based on information about reportable events. Since Secure Computing does not teach all of the limitations of independent claims 2, 26, 43 and 57, those claims should be allowable. Since claims 3-25, 27-42, 44-56 and 58-72 depend from allowable base claims, those claims should also be allowable.

14

At paragraph 19 of the Office Action, the Examiner rejects claims 73-85 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 6,091,835 (Smithies). The Applicant traverses these rejections. Similar to claims 2, 26, 43 and 57, independent claims 73 and 83-85 require an identity authentication code that depends on, "event state data that specifies a condition of the authentication device" (claim 73), "event state data that is a security indicator for an authentication system of which the authentication device is a component" (claim 83), "event state data that specifies information about a user of the authentication device" (claim 84), and "event state data that specifies information about environmental conditions associated with the authentication device," (claim 85).

The Examiner cites claims 1 and 58 of Smithies as teaching the elements of these claims. Similar to the arguments presented above with respect to Secure Computing, the Applicant submits that Smithies does not teach or suggest such an identity authentication code dependent on information about reportable events as required by claims 73 and 83-85. The verification recited in claims 73 and 83-85 involves an identity authentication code that is generated based on information about reportable events (i.e., the event state data), in addition to the conventional inputs for a response computation.

As the Examiner points out, claim 1 of Smithies teaches a computer system for creating a secure, tamper-resistant electronic transcript. Claim 58 of Smithies teaches a computer based system for recording a series of acts constituting the signing of an electronic document and assuring an affirming party's intent. The Applicant respectfully submits that neither claim 1 nor claim 58 of Smithies teaches or suggests the use of an identity authentication code dependent on information about reportable events. Since Smithies does not teach all of the elements of independent claims 73 and 83-85, those claims should be allowable. Since claims 74-82 depend from allowable base claim 73, those claims should also be allowable.
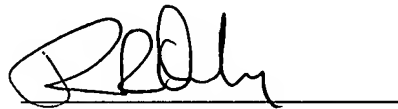
At paragraph 24, the Examiner rejects claims 5 and 11 under 35 U.S.C. 103(a) as being unpatentable over Secure Computing in view of Smithies. However, as set forth above, claims 5 and 11 should be allowable as being dependent on allowable base claims.

Filed herewith is a Request for a Three-Month Extension of Time, which extends the statutory period for response to expire on August 22, 2007. Accordingly, the Applicant respectfully submits that this response is being timely filed.

In view of the above amendment, applicant believes the pending application is in condition for allowance. No other fees are believed to be due in connection with the filing of this response, however the Commissioner is authorized to debit Deposit Account No. 08-0219 for any required fee necessary to maintain the pendency of this application.

Respectfully submitted,

Dated: August 22, 2007

Ronald R. Demsher
Registration No.: 42,478
Attorney for Applicant(s)

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6000 (telephone)
(617) 526-5000 (facsimile)

16